

First, consider the lookup helper in the handlebars Demo. If you look at the server.js file and lookup.handlebars file you will see the following:

```
JS server.js > app.get('/') callback > source4
21
22 app.get('/lookup', (req, res)=>{
23   res.render('lookup',
24     {title: 'lookup helper',
25      user: {
26        username: 'LeeSullivan',
27        age: 20,
28        email: 'hsullivan@stetson.edu'
29      }
30   });
31 })
```

```
views > lookup.handlebars > ...
1 <h2>Handlebars Lookup Helper</h2>
2
3 <p>{{lookup user 'username'}}</p>
4
```

In the server.js file, a user object is created with the fields username, age, and email. The lookup helper returns the object (user) at the index field (username).

Vulnerable Code

Handlebars 3.0.5

Here the code is vulnerable because the lookup function does not properly validate templates.

```
416 instance.registerHelper('lookup', function (obj, field) {
417   return obj && obj[field];
418 });
419 }
```

Secure Code

Handlebars 4.7.7

```
445 define('handlebars/helpers/lookup',['exports', 'module'], function (exports, module) {
446   'use strict';
447
448   module.exports = function (instance) {
449     instance.registerHelper('lookup', function (obj, field, options) {
450       if (!obj) {
451         // Note for 5.0: Change to "obj == null" in 5.0
452         return obj;
453       }
454       return options.lookupProperty(obj, field);
455     });
456   };
457 });
```

```

node_modules 4.7.7 > handlebars > dist > JS handlebars.amd.js > define('handlebars/runtime') callback > template > container > lookupProperty
957 // Just add water
958 var container = {
959   strict: function strict(obj, name, loc) {
960     if (!obj || !(name in obj)) {
961       throw new _Exception['default']('"' + name + '" not defined in ' + obj, {
962         loc: loc
963       });
964     }
965     return container.lookupProperty(obj, name);
966   },
967   lookupProperty: function lookupProperty(parent, propertyName) {
968     var result = parent[propertyName];
969     if (result == null) {
970       return result;
971     }
972     if (Object.prototype.hasOwnProperty.call(parent, propertyName)) {
973       return result;
974     }
975
976     if (_internalProtoAccess.resultIsAllowed(result, container.protoAccessControl, propertyName)) {
977       return result;
978     }
979     return undefined;
980   },
981   lookup: function lookup(depths, name) {
982     var len = depths.length;
983     for (var i = 0; i < len; i++) {
984       var result = depths[i] && container.lookupProperty(depths[i], name);
985       if (result != null) {
986         return depths[i][name];
987       }
988     }
989   }
990 }

```

The following link explains how the code was fixed.

[fix: use String\(field\) in lookup when checking for "constructor" · handlebars-lang/handlebars.js@d541378 · GitHub](https://github.com/defunctzombie/handlebars.js/pull/541)